Defense Logistics Agency Instruction

DLAI 6406
March 26, 2009
Modified October 30, 2009
J-644

Web Site Development and Administration

References: Refer to Enclosure 1.

1. PURPOSE: This Instruction focuses on the DLA Internet process and policy, Section 508 of the Rehabilitation Act, DLA Web development standards, and other technical issues. The processes and policies in this chapter will ensure DLA Web sites and applications comply with public law and higher authority policies; are user friendly, reliable, efficient, and cost effective; and support the warfighter. This chapter is primarily concerned with Nonclassified Internet Protocol Network (NIPRNET) sites. While Secret Internet Protocol Network (SIPRNET) sites must also follow the Electronic Information Access Council (EIAC) process and be 508 compliant, the policies and standards concerning SIPRNET are found on Interlink at www.imd.ismic.gov/interlink_training/beacon.

2. APPLICABIILTY. This instruction applies to all Headquarters (HQ) Defense Logistics Agency (DLA) and DLA Primary Level Field Activities (PLFA) and all DLA Web products designed, developed, procured, or managed by DLA activities and their contractors.

3. POLICY.

a. DLA Web sites must be developed in accordance with the policies and processes prescribed in this document as well as other higher authority documents such as the Deputy Secretary of Defense (DEPSECDEF) memo, “Web Site Administration Policies and Procedures” at http://www.defenselink.mil/Webmasters/policy/DoD_Web_policy_12071998_with_amendments_and_ corrections.html, and Section 508 of the Rehabilitation Act, 29 U.S.C. Section 794d at http://www.section508.gov. This DLA Instruction clarifies and highlights how DLA will meet or exceed higher authority laws and regulations regarding Web site development and administration.

b. Non-.mil Hosting Policy - OMB Memorandum M-05-04, Policies for Federal Agency Public Web Sites, dated December 17, 2004, impacts DLA Web sites and may be viewed at http://www.whitehouse.gov/omb/memoranda/fy 2005/m05-04.pdf. Paragraph 6 stipulates Federal agencies must use .gov, .mil, or Fed.us domains unless the Agency head explicitly determines another domain is necessary for the proper performance of an

Agency function. DLA Information Operations (J-6) strongly endorses this policy for both public and internal Web site hosting. Requests for exemption to the non-.mil hosting policy may be submitted to J-644 via a fact sheet for J-6 Chief Information Office (CIO) approval. A Plan of Action and Milestones (POAM) will be attached to the fact sheet in cases where a temporary exemption is requested.

c. Operations Security (OPSEC) Policy - Effective immediately, no information may be placed on Web sites that are readily accessible to the public unless it has been reviewed for security concerns and approved in accordance with Deputy Secretary of Defense Memo "Web site Administration Policies and Procedures" and, as applicable, DODI 5230.29, "Security and Policy Review of DOD Information for Public Release." Information for public access must be reviewed by personnel trained in (OPSEC).

d. Naming and Addressing Conventions

1) Web site and application names must clearly identify the activity and its organizational linkage to DLA.

2) Publicly Accessible Internet Web Sites – The required convention for HQ's publicly accessible sites is http://www.dla.mil/office or directorate. An example of the address for the J-6 home page is http://www.dla.mil/j-6. The required convention for sites located outside HQ DLA is http://www.unit.dla.mil. An example of the address for the Defense Supply Center Richmond (DSCR) is http://www.dscr.dla.mil.

3) Private, Internal, Restricted, Intranet Web Sites - The required convention is "xxx.dla.mil/DLA staff organization/subordinate levels" for Intranet Web sites. An example of the address for the DLA Today Intranet Web site would be https://today.dla.mil/j-6. An example of the J-64 home page would be https://today.dla.mil/j-6/j-64. An example of the address for DSCR would be https://today.dla.mil/dscr. Intranet Web site addresses typically do not contain "www" unless a waiver is obtained from the DLA EIAC.

e. OMB Memorandum M-05-04, Policies for Federal Agency Public Web Sites, dated December 17, 2004, http://www.whitehouse.gov/omb/memoranda/fy2005/m05-04.pdf, paragraph 6, stipulates Federal agencies must use .gov, .mil, or Fed.us domains unless the Agency head explicitly determines another domain is necessary for the proper performance of an Agency function. J-6 strongly endorses this policy for both public and internal Web site hosting. Requests for exemption to the non-.mil hosting policy may be submitted to J-644 via a fact sheet for J-6 Chief Information Officer (CIO) approval. A POAM will be attached to the fact sheet in cases where a temporary exemption is requested.

f. Must be reviewed and approved by DLA EIAC.

(1) The DLA EIAC is chartered (see J-644 Intranet Library) and authorized to enforce all DLA and higher authority Internet policies.

(2) DLA EIAC review and approval is mandatory for ALL new Web sites and applications for NIPRNET, SIPRNET, and other DLA-sponsored Web sites prior to implementation. Unapproved Web sites including applications (those products which have been implemented without proper approval), must also be submitted to the EIAC for review and approval. J-6 has established an Enterprise portfolio of all DLA Web sites and applications (see below for more info) in an attempt to track every Web project that has been reviewed and approved by the DLA EIAC. DLA EIAC Checklist (see J-644 Intranet Library) – The checklist incorporates relevant Federal, Department of Defense (DoD), and DLA Web development policies and guidelines into a user friendly, convenient, multipoint checklist.

(3) The following policies may be addressed in other documentation such as the higher regulatory authority publications, the DLA EIAC Checklist, and Web development standards, but are highlighted here for convenience and informational purposes:

(a) DLA Logo - All DLA Web sites and applications must have the DLA logo prominently displayed minimally on the home page and login page of the Web site or application. The DLA logo must also be hyperlinked to either http://www.dla.mil, or https://headquarters.dla.mil and http://www.dla.smil.mil on SIPRNET.

(b) Privacy and Security Notice (sample notice at J-644 Intranet Library - Web sites or applications must have a Privacy and Security Notice hyperlink prominently displayed on every Web page. In addition to other required information, the Privacy and Security notice must inform the public that session cookies are being used, what information is being collected and for what reason, and describe the safeguards for handling the information collected from the session cookies. SIPRNET Web sites should follow the Intelink standards and policies for privacy and security notices.

(c) Section 508 Accessibility Statement (sample statement at J-644 Intranet Library) - All DLA Web sites or applications must have a Section 508 Accessibility Statement unless it is determined that compliance would impose an undue burden on the Agency, the system is classified as a national security system, or a compliant product is not commercially available (see paragraphs 3.4., 4.2.2., and 4.6.2. for additional information on Section 508).

(d) Webmaster E-mail Link - All DLA Web sites and applications must have a Webmaster e-mail link, preferably at the bottom of the page. This link is required on every page and/or screen. The Webmaster is responsible for troubleshooting Web site or application technical problems and for ensuring that all system elements work properly.

(e) External Links - All hyperlinks to external, non-Government (not .mil or .gov) resources must clearly support the overall Agency mission or Web site purpose and must present the Agency in a professional manner.

(f) External Link Disclaimer Notice - When one or more external hyperlinks to non-Government Web sites are included on a DLA Web site or application, the Webmaster or content owner is responsible for ensuring that an external link disclaimer notice is made that neither the DOD nor the DLA endorses the product or organization at the destination, nor does the DOD or DLA exercise any responsibility over the content at the destination. This includes credits given to contractors who produce DOD Web sites or applications. An example of an external link disclaimer notice can be found in the DOD "Web Site Administration Policies and Procedures" located at the following link: (http://www.DoD.mil/Webmasters/policy/DoD_Web_policy_12071998_with_amendments_and_corrections.html).

(g) Commercial Software Specification – No commercial logos may be displayed on DLA Web sites and applications. If a document format requires a commercial software product, only text for the software name can be used to reference the document format or hyperlink.

(h) Commercial Advertisements - All DLA Web sites or applications must not contain commercial advertisements, sponsorships, and endorsements unless the site sponsor is a non-appropriated organization as prescribed in the DOD "Web Site Administration Policies and Procedures" at the following link: (http://www.DoD.mil/Webmasters/policy/DoD_Web_policy_12071998_with_amendments_and_corrections.html).

(i) Persistent Cookies - All DLA Web sites or applications are prohibited from using persistent cookies or Web technology which collects user-identifying information such as extensive lists of addresses or other information to identify or build profiles on individual visitors to DLA publicly accessible Web sites. The use of persistent cookies or other Web technologies to collect or store non-user identifying information is authorized only if the Secretary of Defense has personally approved the use of the cookie or technology prior to the implementation of the data collected. Session cookies are allowed.

(j) Contact Us/Feedback - All DLA Web sites or applications must have a "contact us" or "feedback" page or mechanism. The contact us/feedback page will allow user comments and feedback to be directed to the functional point of contact.

(k) Private Links on Publicly Accessible Web Sites - All publicly accessible DLA Web sites or applications must not contain links or references to DLA Web sites with security and access controls (e.g., internal, restricted, private Web sites such as Intranets). Under rare circumstances, it may be appropriate to establish a link to a restricted site provided details as to the controlled site's content are not revealed.

(l) External Hosting of DLA Web Sites - All DLA activities will use existing DLA Internet and Intranet hosting services and support unless requirements clearly justify external hosting services and support. External hosting services must be approved by the DLA CIO, J-6. The process for requesting a waiver from mandatory DLA hosting service and support is to submit a fact sheet to the DLA EIAC. The DLA EIAC will review the waiver request and will provide a recommendation to the CIO. The DLA CIO will decide whether to approve or disapprove the external hosting waiver request.

(m) Scientific and Technical Information Network (STINET) Registration – All DLA Secure Hypertext Transfer Protocol (https:) Web sites must be registered in the "DOD Restricted Information Sources" registry which is not publicly accessible. This registry can be accessed on the Defense Technical Information Center (DTIC) Secure STINET (S-STINET) (http://stinet.dtic.mil/info/s-stinet.html).

(n) Defense Information Technical Center Search (DTIC Search) – All DLA Web sites representing mission areas, staff organizations, and field activities are required to be registered in the DTIC Search. Webmasters will register the appropriate information to the DTIC Search at (http://www.dtic.mil/dtic/search/DoD_search.html), which hosts the DOD Web Site Registration System. Upon receipt of the DTIC Search record, the DTIC Search administrator will link the site to Defense LINK. Webmasters will add, update, and delete DTIC Search records, as required.

(o) Web Broker System (WEBBS) - WEBBS is an existing HQ DLA Web application tracking system that includes the DLA Enterprise portfolio of all Web projects.

g. Section 508 Policy: DLA must comply with all applicable provisions of Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220), (http://www.section508.gov/index.cfm?FuseAction=Content&ID=12) when developing, procuring, maintaining, or using electronic and IT unless it is determined that compliance would impose an undue burden on the Agency, the system is classified as a national security system, or a compliant product is not commercially available.

h. Web Development Standards:

(1) All DLA Web sites and applications will be designed and developed in accordance with the standards prescribed below. DLA Web development standards are available in the J-644 Intranet Library and include:

(a) Web Design Standard (SCM-STA.DE.6000) - policies, procedures, and guidelines for designing, developing, and maintaining DLA Web sites and applications. A standard design for all DLA public and Intranet sites is intended to meet the following objectives: (1) facilitates 508 compliancy, (2) facilitates a corporate brand, (3) facilitates user-friendly Web sites (e.g., consistent design across all sites), (4) makes content management easier (e.g., fill a Web form vs. Frontpage), (5) content management systems will be implemented based on the standard, and (6) more efficient and saving time and money.

(b) Web Development Coding Standard (SCM-STA.CD.6000) - policies, procedures, and guidelines for the development and sustainment of DLA Web applications and ensures Web products are Section 508 compliant.

(c) Web Development Database Standard (SCM-STA.DA.6000) - policies, procedures, and guidelines for establishing, developing, operating, and maintaining relational databases used by DLA Web applications.

(2) Related Standards and Documentation - All DLA Web sites and applications are subject to the policies and processes contained in publications such as DOD Directive 8000.1, Management of DOD Information Resources and Information Technology (http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf) and DLA Instruction, Automated Information System (AIS) Life Cycle Management (LCM) Oversight/Guidance Contemporary/Legacy Systems. These policies and processes ensure the design, development, deployment, operation, maintenance, enhancement, and retirement of information products is managed throughout their life cycle. An LCM model is especially critical for Web applications and is mandatory. J-64 has created an Internet Development Life Cycle (iDLC) model, mirrored after the Capability Maturity Model Integrated, but specifically tailored for the rapid Web development world. Each phase of the software development process has potential documentation which may be used. The J-6 iDLC Library is available on the J-644 internal web site. The iDLC Reference Document is recommended for initial review as it provides a high-level overview of the J-6 iDLC model. The program manager (PM) is responsible for ensuring the Web development coding and database standard is followed.

i. Information Security, Public Affairs, and Privacy.

(1) Classified Information - Under no circumstance will classified information be placed on, or made accessible by, DLA public Web sites, unsecured Web sites, or NIPRNET Intranet sites.

(2) For Official Use Only (FOUO) - Information that requires special handling, contractor proprietary data, procurement-sensitive information, and products with specific licensing or restrictions) should not be available to the general public.

(3) Public Affairs - Information posted to public Web sites must be managed in accordance with DOD Directive 5230.9 and DODI 5230.29. The DLA Public Affairs Office is responsible for establishing a process to review, approve, and monitor all public Web page content for the Agency. By definition, information on a DLA Intranet is not available to the public and does not require approval by DLA Public Affairs Office.

(4) Privacy Information - All DLA Web sites must follow privacy guidelines which prohibit the display of privacy information without DLA Privacy Official approval.

j. Information Assurance (IA).

(1) DLA Web projects will be certified and accredited in accordance with DODI 5200.40, DOD Information Technology Security Certification and Accreditation Process and DLA Policy. Relevant DLA IA policy and processes are described in the following DLA Instructions:

(a) IA Management Controls

(b) IA Operational Controls

(c) IA Technical Controls

(d) IA Rules of Behavior

(2) IA Computer Emergency Response Team (CERT) (http://www.us-cert.gov/) – All applications, including hardware and software, that support DLA Web sites, will implement required mitigation actions identified via Information Assurance Vulnerability Alerts (IAVA), taskings, and advisories. IAVAs may be reviewed at http://www.us-cert.gov/. Some of the more significant Web development IAVAs are included here as a convenience (please refer to the link above for the most up-to-date guidance).

(a) Cross-Site Scripting - All DLA Web sites or applications must prevent cross-site scripting vulnerabilities (http://www.cert.org/advisories/CA-2000-02.html).

(b) Malicious Content Mitigation - All DLA Web developers and Webmasters must incorporate the findings from “Understanding Malicious Content Mitigation for Web Developers” (http://www.cert.org/tech_tips/malicious_code_mitigation.html) into coding practices.

(c) Mobile Code - All DLA Web developers and Webmasters must understand the DOD Mobile Code Technology guidelines (http://www.dtic.mil/whs/directives/corres/pdf/855201p.pdf) and ensure all development efforts are minimally compliant with the DOD Mobile Security Technical Implementation Guide as well as all approved DOD Instructions issued by the Office of the Assistant Secretary of Defense for Networks and Information Integration/DOD CIO.

(d) Structured Query Language (SQL) Injection Prevention – All DLA Web developers and Webmasters must prevent SQL injection vulnerabilities that allow database users to leverage administrative privileges on a single database to execute SQL queries or operating system commands with greater privileges (http://www.kb.cert.org/vuls/id/508387).

4. RESPONSIBILITIES. Refer to Enclosure 2.

5. PROCEDURES. Refer to Enclosure 3. Definitions are located in Enclosure 4 and Additional Information is located in Enclosure 5.

6. EFFECTIVE DATE. March 26, 2009

Director, DLA Enterprise Support

5 Enclosures
Enclosure 1 – References
Enclosure 2 - Responsibilities
Enclosure 3 - Procedures
Enclosure 4 – Definitions
Enclosure 5 – Additional Information

Enclosure 1
References

1. Section 508 of the Rehabilitation Act Amendments of 1998 (Public Law 105-220, 29 U.S.C. 794(d) (http://www.section508.gov).

2. Title 5, U. S. Code, Section 552, "Freedom of Information Act" (http://frWebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+5USC552).

3. Title 5, U. S. Code, Section 552a, "The Privacy Act of 1974" (http://frWebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+5USc552a).

4. Title 10, U. S. Code, Section 130b, "Personnel in Overseas, Sensitive, or Routinely Deployable Units," (http://frWebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+10USC130b).

5. E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch 36) (http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR02458:|TOM:/bss/d107query.html or http://frWebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf).

6. 39 CFR Part 1194, "Electronic and Information Technology Accessibility Standards" (http://www.access-board.gov/508.htm).

7. 48 CFR 39, "Federal Acquisition Regulation; Section 508 Micropurchase Exception Sunset Provision" (http://www.acqnet.gov/far/FAC/fac2001-11.pdf).

8. Federal Acquisition Regulation (FAR), "Final FAR Rule For Implementing Section 508 of the Rehab Act Electronic and Information Technology Accessibility for Persons with Disabilities" (http://www.section508.gov/index.cfm?fuseAction=Content&ID=13).

9. OMB Memorandum M-05-04, Policies for Federal Agency Public Web Sites, dated December 17, 2004, (http://www.whitehouse.gov/omb/memoranda/fy2005/m05-04.pdf).

10. DEPSECDEF Memo: Web Site Administration, Policies and Procedures (http://www.defenselink.mil/Webmasters/policy/DoD_Web_policy_12071998_with_amendments_and_corrections .html).

11. SECDEF Memo Information Security/Web Site Alert (http://www.defenselink.mil/Webmasters/policy/infosec20060806.html).

12. DOD 5200.1-R, DOD Information Security Program Regulation, January 1997, (http://www.dtic.mil/whs/directives/corres/pdf/520001p.pdf).

13. DOD Directive 8500.1, Information Assurance, October 2002, (http://www.dtic.mil/whs/directives/).

14. DODI 8500.2, Information Assurance Implementation, February 6, 2003, http://www.dtic.mil/whs/directives/).

15. DODI 5200.40, DOD Information Technology Security Certification and Accreditation Process, (DITSCAP), December 30, 1997, http://www.dtic.mil/whs/directives/).

16. DOD Manual 8510.1M, DOD IT Security Certification and Accreditation Process (DITSCAP) Application Manual, July 2000 (http://www.dtic.mil/whs/directives/).

17. DOD Directive 8000.1, Management of DOD Information Resources and Information Technology, March 2002, (http://www.dtic.mil/whs/directives/).

18. DOD Directive 5230.9, Clearance of DOD Information for Public Releases, April 1996, (http://www.dtic.mil/whs/directives/).

19. DODI 5230.29, Security and Policy Review of DOD Information for Public Release, August 1999, (http://www.dtic.mil/whs/directives/corres/html/523029.htm).

20. DOD 5500-7R, DOD Joint Ethics Regulation, (particularly Chapter 2, Section 301, Use of Government Resources), (http://www.defenselink.mil/DoDgc/defense_ethics/ethics_regulation/jer1-4.doc).

21. Privacy Act (http://www.usdoj.gov/oip/privstat.htm).

22. DLA FOIA Program (http://www.dla.mil/public_info/efoia/dlafoiaregs.html).

23. FOUO Material.

24. Personnel Records and Files Systems.

25. AIS LCM Oversight/Guidance Contemporary Legacy Systems.

26. IA Technical Controls.

27. External Web Sites.

28. IA Management Controls.

29. IA Operational Controls.

30. IA Rules of Behavior.

31. DLA Information Technology Standards, and DLA Information Technology Solutions, for hardware architecture compliance. (http://sirnet.metamatrix.se/material/SIRNET_08/technical_standards_0104.pdf).

Enclosure 2
Responsibilities

1. DLA EIAC Process:

a. DLA Web developers (Government and contractor) must be knowledgeable of all applicable policies and standards PRIOR to beginning development of a Web site or application and will consider these requirements when designing the Web product.

(1) Review and implement all policies, standards, mechanisms, and process controls in this DLA Instruction . A recommended order of precedence is: AIS LCM model to manage the project life cycle, IAVAs, Web development standards, DLA EIAC Checklist, and DLA EIAC review and approval.

(2) Pursue training opportunities to fill any knowledge gaps meeting these requirements.

(3) If assistance is required, contact the EIAC or J-644 at Webmaster@dla.mil.

b. New or updated Web products or applications will be submitted to the DLA EIAC for review and approval.

(1) Local Site Approvals:

(a) IA Reviews - The process for reviewing a Web site (i.e., static HTML pages) is different from a Web application (i.e., database-driven site) and the two processes are outlined below:

[1] Web Site - The local Information Assurance Officer (IAO) and Information Security Officer will conduct a basic review and approve the site's submission to the DLA EIAC. The basic review will ensure that no sensitive or inappropriate information is presented on the Web site without appropriate safeguards.

[2] Web Application - Web applications are considered systems and require a more in depth review process. The local IAO will ensure all requisite tasks associated with the DIACAP, http://www.dtic.mil/whs/directives/. are accomplished in order to certify and accredit a Web application.

(b) Other local expert representatives from organizations such as legal, security, contracting, customer service, and others may periodically be requested to participate in a Web site review, if necessary.

(c) If the Web site or application utilizes a software or hardware component/tool which is not in the DLA IT Solutions document (see J-644 Intranet Library) and local Configuration Control Board (LCCB) list of approved products, those appropriate reviews and approvals must be obtained prior to DLA EIAC review. The Information Technology Solutions Adoption Process is prescribed as a separate policy.

(d) Certification by the local DLA IT Solutions Director, or site Webmaster, is required.

(2) All new, previously unapproved, or renovated Web products, applications, and repositories will be submitted through the IT Change Request (ITCR) Front Door system. The Project Manager or point of contact (POC) for the Web product must certify that they have reviewed and approved the product prior to submitting to the ITCR.

(a) J-644 WPT conducts an informal review with the EIAC Checklist and identifies items which do not comply with policy. J-644 WPT provides a summary of the informal review findings to the PM/Webmaster for reconciliation. The PM/Webmaster notifies J-644 when items are reconciled for a final confirmation review.

(3) J-644 WPT submits the site to the DLA EIAC for formal review and approval.

(a) The DLA EIAC review process includes representatives from the Public Affairs Office, Privacy/FOIA, Information Security, OPSEC, one GS-15/0-6 from each J-6 Code and Headquarters staff area, and one GS-14/0-5 from each field site.

(b) Members provide feedback on the Web site and recommend approval or disapproval. Approval may be contingent upon changes being made to the site and J-644 WPT will ensure changes are implemented. A majority of all members must approve the Web site or application in order to receive EIAC approval. The DLA EIAC review process averages 4 weeks, depending upon the size and scope of the Web project, and number of errors which must be corrected. In the event that a delay will negatively impact a deadline, the review process can be expedited.

(c) If approval is received from the DLA EIAC, J-644 WPT notifies the site sponsor and Council members. A summary of findings may be provided by J-644 WPT. If approval is not recommended, site sponsor and members are notified what actions are required to receive approval. The Web site will NOT be placed into production until approval is received.

(d) In the event that approval from the voting members of the DLA EIAC cannot be achieved, J-644 will provide a summary of the issues and a recommendation to the DLA CIO and the DLA CIO will make a final decision on whether the site may be approved and implemented.

(e) The J-6 CIO may remove or block access to any application/site that moves to production without approval from the EIAC.

c. All DLA-sponsored Web sites or applications will be reviewed periodically (e.g., annually) by the site sponsor and Webmaster and randomly by J-644 WPT, for compliance with DLA and higher authority policies.

(1) The site sponsor and their technical support are responsible for periodically reviewing their Web products to ensure they remain in compliance with all regulatory policies.

(a) The Web site sponsor can dispute DLA EIAC and J-644 WPT findings. J-644 WPT will review disputed items and release findings to the site sponsor.

(b) If the site sponsor agrees with the J-644 WPT findings, the site sponsor and/or their Webmaster are responsible for implementing suggested changes. J-644 WPT will assist Webmasters and developers as much as possible.

(c) If the Web site or application changes are not implemented or are not included in future redesign plans, the J-644 WPT will escalate the situation to the DLA EIAC Chairperson. The EIAC Chairperson has the authority to take steps to remove the violating Web site from the DLA domain. The Chairperson may consider escalating controversial issues up the J-6 management chain, ultimately to the J-6 CIO for resolution.

Enclosure 3

Procedures

1. Section 508 Process:

a. Section 508 and Electronic and IT Procurement - Procurement officials and Webmasters are knowledgeable of all applicable Section 508 standards prior to electronic and IT procurement. Market research should be conducted to identify the product that is most compatible with Section 508 and product or system requirements.

(1) Section 508 Exemption - The market research process and design phase will determine whether or not the electronic and IT procurement is exempt from 508 due to an undue burden, national security system, or commercial nonavailability. A tool to assist during the market research stage is the General Services Administration's (GSA) Buy Accessible Wizard (http://www.buyaccessible.org). Prior to purchase, if a product is not listed in the Buy Accessible Wizard, ask the vendor or developer to fill out a Voluntary Product Accessibility Template (VPAT) (http://www.section508.gov or http://www.itic.org/policy/508/Sec508.html).

(a) Market research or the product design phase may determine that the product is exempt from Section 508 compliance due to the following reasons: commercial nonavailability, making the product Section 508 compliant would be an undue burden to the Agency, or the system is a national security system, the exemption status must be documented with the J-644 WPT. If a product is not compliant with Section 508, the Agency is still required to provide alternative access to the information to individuals with disabilities.

(b) Section 508 requires that the Agency must retain records of all Section 508 exemptions granted. Contact the J-644 WPT to obtain the Section 508 Exemption templates (see J-644 Intranet Library). The Requiring Official must explain why the system falls into a Section 508 exemption category. A thorough rationale is required. Explanations must be adequate to survive protests and litigation challenges.

(c) Submit the completed Section 508 Exemption template to the J-644 WPT for final approval.

b. Section 508 in the Web Development Process – Developer is knowledgeable of all applicable policies and standards of Section 508 PRIOR to beginning development of a Web site or application and considers these requirements when designing the Web product.

(1) Review and implement DLA Enterprise practices for Section 508 in the DLA Web Development Coding Standard (see J-644 Intranet Library).

(2) Development Phase and Section 508 – Success meeting Section 508 requirements is ensured if considered and planned for in the development phases of a Web product. For example, a developer can code Section 508 requirements throughout the Web product development or immediately prior to production implementation. Some developers use Dreamweaver's™ accessibility features to insert alt tags and other basic 508 requirements throughout the development process. Others prefer to code for Section 508 as a final step in the development process. Either approach is acceptable as long as Section 508 requirements are met.

(3) Web products must go through Section 508 testing prior to production. Verification for compliance can be done through peer reviews (e.g., alternate developer or project manager) and verification software.

c. Section 508 Review - All Web sites, applications, and multimedia presentations will be reviewed periodically) by the Web site sponsoring office, Webmaster, and J-644 WPT to ensure Section 508 compliance is required prior to EIAC approval.

(1) Review Steps – Verification of compliance with Section 508 requires two methods, algorithmic and human judgment. The algorithmic method uses automated software tools, such as AccVerfiy™ or AccMonitor™, to test whether or not Section 508 checkpoints (a) through (p) requirements are satisfied within the code. Human judgment is also necessary to translate broad requirements such as usability which meet the spirit of Section 508 for impaired individuals.

(2) Web site sponsoring office and Webmaster are responsible for ensuring the Web product remains compliant with DLA and higher authority policies at all times. At a minimum, a Web product review will be conducted annually.

(3) Site POCs will review Web sites annually for compliance with DLA and higher authority policies. The Web site or application will be considered noncompliant until all violations are resolved. If the Web site or application changes are not implemented or are not included in future redesign plans, the J-644 Web Policy Team will escalate the situation to the DLA EIAC Chairperson. The EIAC Chairperson has the authority to take steps to remove the violating Web site from the DLA domain. The Chairperson may consider escalating controversial issues up the J-6 management chain, ultimately to the DLA CIO for resolution.

Enclosure 4
Definitions

Alternative Format. Alternate formats usable by people with disabilities may include, but are not limited to, Braille, American Standard Code for Information Interchange (ASCII) text, large print, recorded audio, and electronic formats that comply with Section 508 requirements.

Alternative Method. Different means of providing information, including product documentation, to people with disabilities. Alternate methods may include, but are not limited to, voice, fax, relay service, TTY, Internet posting, captioning, text-to-speech synthesis, and audio description.

Assistive Technology. Any item, piece of equipment, or system, whether acquired commercially, modified, or customized, that is commonly used to increase, maintain, or improve functional capabilities of individuals with disabilities.

Content Owner. A content owner (also may be referred to as Web author) is the person or organization in charge of developing and approving Web site content prior to posting on the Internet or Intranet. The content owner must be knowledgeable of all policies governing appropriate Web site content.

Commercial Nonavailability. Refers to circumstances where no commercial items are available that meet the applicable Access Board’s technical Section 508 provisions (directly or through equivalent facilitation) in time to satisfy the Agency’s delivery requirements.

Cookie. A "cookie" is a small piece of information (token) sent by a Web server and stored on a user’s system (hard drive) so it can later be read back from that system. Using cookies is a convenient technique for having the browser remember some specific information. Cookies may be categorized as "session" or "persistent" cookies.

Electronic and Information Technology (E&IT or EIT). IT and any equipment, or interconnected system or subsystem of equipment that is used in the creation, conversion, or duplication of data or information. This includes computers, ancillary equipment, software, telecommunication products, such as telephones, information kiosks, World Wide Web (WWW) sites, multimedia, and office equipment.

FOUO. Material that must not or should not be publicly disclosed because some harm would or could result from the disclosure. All FOUO information must be secured by login and password access restrictions regardless of whether the information is publicly or privately accessible.

Internet. A collection of worldwide “network of networks” that use the transmission control protocol/interface protocol (TCP/IP) for communications. The Internet includes resources that span academia, business, Government, and personal interests. (NOTE: Internet sites are considered “public” and will be used by non-.mil and non-.gov users such as members of the public, contractors, etc.)

Intranet. A site and/or server that uses security or access controls to strictly limit access to users from within an Agency, organization, or company. Access controls include various security features such as firewalls, domain/IP restrictions, common access cards, and other methods of authentication and restriction. (NOTE: Intranet sites are considered “internal” and “restricted” and will be used by authorized military and Government users. Intranet sites are typically used to support business operations of the Agency).

National Security System. EIT used by agencies involved in intelligence activities, cryptology equipment supporting national defense, command and control of military forces, mission critical military or intelligence systems, and equipment that is an integral part of a weapon or weapon system.

Persistent Cookies. Cookies that remain over time and can be used for a variety of purposes including to track a user's access over time and across Web sites or to establish user preferences.

Section 508 of the Rehabilitation Act. Section 508 of the Rehabilitation Act requires that any electronic and IT developed, procured, maintained, or used by the Federal Government be accessible to persons with disabilities.

Service Oriented Architecture (SOA). SOA is a software architectural concept that defines the use of services to support business requirements. SOA resources are made available to other participants in the network as independent services that are accessed in a standardized way. Most definitions of SOA identify the Web services using Simple Object Access Protocol (SOAP) and Web Service Description Language (WSDL) in its implementation; however, it is possible to implement SOA using any service-based technology.

Session Cookies. Session cookies are temporary cookies that are used to maintain context or "state" between otherwise stateless Web transactions (e.g., to maintain a "shopping basket" of goods selected during a single logical session at a site) and that must be deleted at the end of the Web session in which they are created.

Undue Burden. Undue burden means significant difficulty or expense. In determining whether an action would result in an undue burden, an Agency shall consider all Agency resources available to the program or component for which the product is being developed, procured, maintained, or used. The Agency is still required to provide alternative access to the information, and document the undue burden in the contracting file.

VPAT. The VPAT is a standard template that a vendor can copy and fill-in product information to describe how a particular product or service they offer conforms to Section 508 Access Board standards.

Web Application. A Web application is a dynamic, database-driven program that may be separate and distinct from the parent Web site or contained within the parent Web site, and may consist of a thin-client (the Web browser), a presentation tier (Web server), an application tier (application/component server), and a database (database server).

Webmaster. A technical individual that manages a Web site. Depending on the size of the site, the Webmaster might be responsible for any of the following: (1) Designing the Web site, (2) creating and updating Web pages, (3) replying to user feedback regarding Web site functionality, (4) and monitoring Web site traffic. In some instances, the Webmaster may also be the content owner.

Web Page. A page of information typically presented using HTML and accessible using the WWW. Web pages may present a variety of information sources from text to a combination of sound, graphics, and video.

Web Services. Web services use open standards to allow connectivity across networks and the internet and facilitate interoperability and data exchange:

- Messaging protocol, SOAP
- Transport protocols (including HTTP, HTTPS, JMS)
- Security can be handled at both the transport level (HTTPS) and/or at a protocol level (WS-Security)
- Web Service Definition Language (WSDL) allows Web services to be self-describing for a loosely coupled (modular) architecture and have providers and consumers
- Standards bodies, including WSI, W3C, and OASIS exist using technologists from industry leading software vendors

Web Site. A collection of information organized into a number of Web documents related to a common subject or set of subjects, including the "home page" and the linked subordinate information. A Web site generally has a unique functional sponsor, which can be different from the parent site it is hosted with.

Example of Web site and subordinate Web site. DLA Home Page (www.dla.mil) is a Web site sponsored by the Public Affairs Office, primarily consisting of the top layer files such as About DLA, News, Library, etc. There are several subordinate Web sites under the DLA Home Page such as J-6, J-8, DES, etc., which are separate and distinct from the parent DLA Home Page site and each have a different functional sponsor.

Web System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information that require more than $1M per year to maintain.

The term “Internet” or “Intranet” may be used interchangeably throughout this document. The difference between an Internet and Intranet site is the former site is publicly accessible while the latter is restricted via security and access controls (e.g., .mil restricted or login required).

The term “developer” or “Webmaster” may be used interchangeably throughout this document. Both the developer and Webmaster have key roles in developing and maintaining Web sites and applications. The difference between a developer and Webmaster is that a developer may be involved as a Web programmer whereas a Webmaster is involved primarily with Web site design and content management.

The term “site,” “application,” or “product” may be used interchangeably throughout this document. The difference between site and application is that a site contains static HTML files while applications are dynamic and database driven. A product can be either a site or an application.

Enclosure 5

Additional Information

The outputs of Web development related processes are:

a. DLA EIAC: DLA Web sites and applications that comply with all Federal, DoD, and DLA policies.

b. Section 508: DLA Web sites and applications which are accessible to all citizens and employees with disabilities and compliant with Section 508 requirements.

c. Web Development Standards: Web sites and applications must adhere to DLA Web development standards. Development standards benefit the Agency by: (1) increasing productivity and enhancing efficiency, (2) reducing costs over the product life cycle, (3) facilitating interchangeability of Information Technology (IT) products, (4) increasing quality assurance, and (5) facilitating teaming and flexibility within the Agency because common skill sets may be shared. Project managers will work with developers and other participants (e.g., analysts) to ensure compliance with these standards. DLA Web development standards are available in the J-644 Intranet Library.